SOCIAL ENGINEERING – ÉS AMI MÖGÖTTE VAN

Megtévesztők

CD1/DVD
A cikkben említett programok megtalálhatók a lemezmellékleten

Sorozatunk ötödik epizódjában a megtévesztésről és az ellene használható védekezési módszerekről lesz szó, de megtudhatjuk azt is, mi az a PhishTank, és többek között felvázolunk egy nagy csokor hasznos védelmi tippet.

A veszély az emberiséggel egyidős. Mindig is voltak a természetben ellenségeink, ráadásul rosszindulatú embertársaink is régóta velünk élnek. Ők lelkiismeret-furdalás nélkül kihasználták, kifosztották a tapasztalatlanabbakat, a gyengébbeket. Az informatika korában ez úgy jelentkezik, hogy sok, magas szintű – de legalábbis átlag feletti – számítástechnikai tudással felvértezett (nem utolsósorban kiváló emberismerettel megáldott) vírusíró és csaló úgy érzi, joga van tudatlan áldozatait becsapni, meglopni, megkárosítani, akik ezt sokszor szinte észre sem veszik. Az utóbbi évek tendenciája azt bizonyítja, hogy míg kezdetben elsősorban virtusból és kitűnni vágyásból készítettek kártékony kódokat, mára ez elsősorban üzleti céllal végrehajtott bűncselekménnyé lépett elő. A reklámterjesztők fizetnek a víruskészítőnek a fertőzött gépekről kiküldött kéretlen reklámokért (spam), bérbe veszik a távirányítható fertőzött gépekből álló botnethálózatot, de eladható internetes portékává léptek elő a trójai és kémprogramok segítségével ellopott hitelkártya- vagy személyes adatok is. Ezek mellett olyan internetes csevegőszobák (chatrooms) is léteznek, melyekben az adathalászok, botnet-„pásztorok" nyíltan hirdetik szolgáltatásaikat.

Őrködni kell a javak felett

Ahogy gépkocsinkat vagy lakásunkat sem hagyjuk tárva-nyitva magunk után, úgy kétségtelenül számítógépünknek is szüksége van hathatós védekezésre.

A statisztikák szerint jelentős mennyiségű károkozó program mindig arra a számítógépes környezetre készül, amelyet egyrészt tömegesen használnak, másrészt széleskörűen hozzáférhető technikai dokumentációval is rendelkezik. Ez jelenleg – az egyszerű felhasználók szempontjából – döntő többségben a windowsos asztali rendszereket jelenti, de semmiképpen sem mondhatjuk, hogy a többi platform teljesen mentes lenne a támadásoktól. A kártevők összezavarhatják a számítógépet, tönkretehetik a benne tárolt adatokat, és sajnos az sem kizárt, hogy bizalmas adatainkat, valamint a használat során alkalmazott kódokat illetéktelenek részére juttatják el, amelyekkel vissza is élhetnek.

Ám a megfelelő védelmi program és a frissítés csak a szükséges megoldás egyik fele. A másik oldalon a józan észnek, az óvatosságnak kell(ene) erőteljesen munkálkodnia. Murphy szerint „Bízz embertársadban, de azért emeld meg a kártyapaklit!" Mivel az internet világát bizonyíthatóan nem csupa Grállovag népesíti be, szükséges az egészséges, józan gondolkodás, a rendszeres kételkedés. Mára már elkerülhetetlen, hogy az átlagemberek megszabaduljanak a naivitástól, a túlzott jóhiszeműségtől. Vesztenivalója igenis mindenkinek van, nem intézhető el egy kézlegyintéssel: „ugyan ki támadna éppen engem, hiszen én jelentéktelen szürke célpont vagyok!" A megfelelő hozzáállást talán éppen Senecától leshetjük el: „Aki mindenkiben megbízik, az éppolyan káros, mint aki senkiben sem." Kell tehát egy alapértelmezett egészséges bizalmatlanság ahhoz, hogy később ne váljunk áldozattá. Ezt minimális informatikai tájékozottsággal már alapszinten elérhetjük – ehhez olvassunk időnként számítástechnikai és biztonságtechnikai témájú weboldalakat, magazinokat.

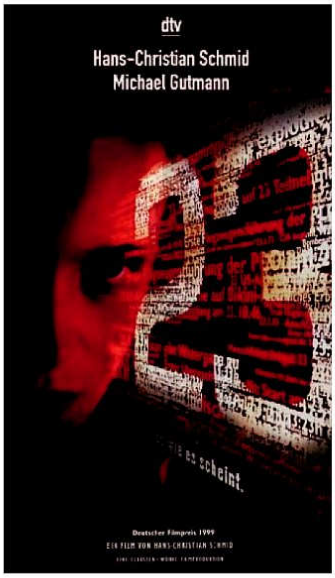
Archetípusok - fő felelős az emberi természet

A tanmesében a farkas magát a kecskemamának kiadva kopogtat a kecskecsalád ajtaján, ahol az egyedül lévő kisgidák, távol lévő anyjuk tanácsát követve, arra kérik, először mutassa meg a mancsát, fehér-e – hát persze, hogy nem az! A farkas hoppon marad - ám nem adja fel, cselhez folyamodik. A furfangos ordas lisztbe meríti a mellső lábát, majd krétát nyel, és úgy megy vissza újra. Mivel a lába ezúttal már fehér, és a hangja is vékony, hát a kisgidák beengedik, a történet folytatását pedig már valamennyien ismerjük. Nos, a számítógép-használók többsége még ilyen minimális figyelmet sem fordít saját biztonsága megóvására. Újból és újból megjelennek a kéretlen levelek (spam) – a mellékletben digitális kártevőkkel – és mindig a felhasználók naivságára, kíváncsiságára apellálnak – sikerrel.

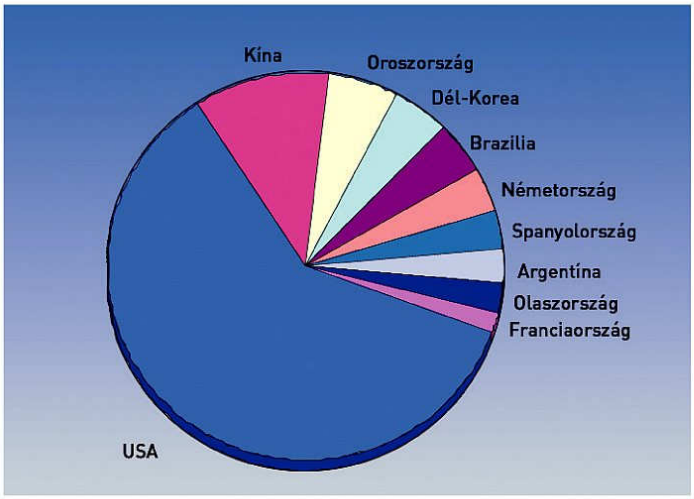
Kurnyikova meztelen fotói, gyors haszon a tőzsdén, különleges gyógyszerakció, azonnali adó-visszatérítés, Vista crack, kiemelkedő jövedelem napi egy óra otthoni munkával, univerzális szériaszám-generátor minden vírus-keresőhöz, férfiasságnövelő, ingyendiploma, csodás fogyókúrarecept, 230 halottja van az Európában dúló viharoknak, keresik a balesetben elhunyt milliomos örökösét, és küldjük el az összes személyes adatunkat – az ismeretlenektől érkező levelek típusainak felsorolása még hosszan folytatható.

Vajon Diane Clara igazán azt gondolja, hogy 30 dollárért meg fogjuk venni a gyógyfüvekből készült pénisznövelő piruláit? És vajon az állítólagos Ibro Usen, a Bank of Africa könyvvizsgálati és könyvelési szekciójának munkatársa Burkina Fasóban valóban át-

Micsoda különbség! – mondhatnánk. És valóban, a csaló oldal még a PIN-kódunkat is bekéri – korántsem véletlenül



Az egyik első film, amely hackerekről szól, valóságon alapuló történettel



Továbbra is az USA a trójai és billentyűzetnaplózó programok fő kibocsátója

2006 DDoS, vagyis távoli szolgáltatásmegtagadásos támadásai

A személyes adat érték, ne szórjuk magunkról bőkezűen az információkat a közösségi portálokon

utalja majd takarékbetét-számlánkra azt a 9 millió dollárt, ha megadjuk a személyes banki adatainkat? Amíg van, aki ezt elhiszi, nem lehet teljesen útját állni a csalásoknak. Sajnos mindig akad kellő számú balek, akik miatt a rosszfiúknak megéri trükközni.

Át a palánkon - egy korai adathalász akció

A tipp régi: a 23 című filmben (1998, rendezte Hans-Christian Schmid) a főszereplők Németországban C64 és Atari gépekkel törnek be különböző számítógéprendszerekbe (a Karl Kochról szóló film valóságos eseményeken alapul, fiatalok egy csoportja ténylegesen betört egy nukleáris erőmű rendszerébe). Az ötlet már ott is elhangzott: hogyan lehet betörni oda, amit nagyon őriznek? Hát fel kell állítani egy hamis kaput, amely igazinak látszik, abba beírják az adatokat a gyanútlan belépők, utána a látszat kedvéért azért továbbítani kell őket az igazi bejárathoz is, nehogy gyanakodjanak, de az adatok máris a mi kezünkben vannak.

Adathalászat (Phishing)

Az adathalászat során internetes csalók e-maileket küldenek szét fontos cégek (például bankok, hitelintézetek, közhivatalok) nevében, hogy megtévesztve a címzetteket, hozzáférjenek azok bizalmas adataihoz, például hitelkártyaszámokhoz, jelszavakhoz. Ezek a trükkös üzenetek például felhívják a felhasználó figyelmét arra, hogy látogasson el egy internetes honlapra, ahol azután személyes adataik beírására utasítják, azzal az ürüggyel, hogy frissítik az információkat, de akár meg is fenyegethetik, hogy zárolják számlájukat, ha nem mennek el az adott weboldalra. Ami azonban első pillantásra a vállalat hivatalos honlapjának tűnik, az nem más, mint a csalók által létrehozott tökéletes másolat. Ha valaki itt megadja számlájának részletes adatait, arra már keresztet is vethet: a csalók rekordsebességgel megcsapolják azt. A machináció lényege, hogy megtévesztéssel fontos információkat csaljanak ki valakitől.

Az adathalászat az úgynevezett Social Engineering tevékenységek családjába tartozik: ez egy szépen hangzó elnevezés, valójában azonban olyan manipulációt jelent, amelynek segítségével, hamis látszattal olyan dolgokra is rávehetők az emberek, amilyenekre megtévesztés nélkül nem lenne esély. Újabban előfordulnak hamis telefonszámmal való visszaélések is, ilyenkor a bank nevében a csalók várják „adategyeztetésre" az ügyfeleket. Meghaladja a cikk terjedelmét a számos – sajnos életszerű és hihető – példa, amit Kevin Mitnick könyveiben olvashatunk, ezért csak egyetlen példát ragadunk ki: „Halló! Jó napot kívánok, én a rendszergazda vagyok, éppen rendszerátállás van, kérem, diktálja be gyorsan a jelszavát..." Akit bővebben is érdekel, mindenképpen olvassa el a Megtévesztés művészete és a Behatolás művészete című, magyarul is megjelent izgalmas köteteket.

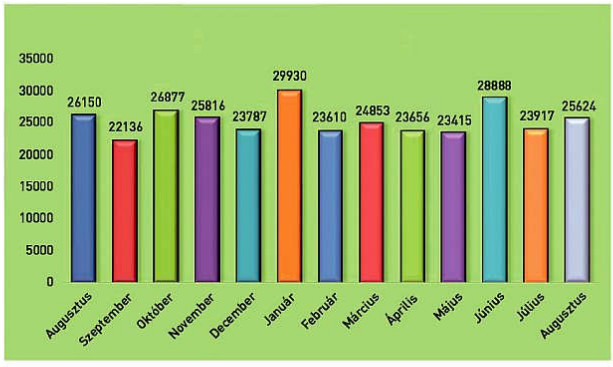
Célkeresztben az átlagember

Identity theft – azaz személyiséglopás. Mit értünk ezen? A személyiség (személyes adatok, kapcsolatok) eltulajdonítását, valamilyen tisztességtelen szándékkal. Ez régóta létezik (gondoljunk csak az ellopott útlevelek, jogosítványok, igazolványok vagy akár a jövedéki zárjegyek feketepiacára), a modern technológia azonban új távlatokat nyitott meg az elektronikus forma előtt. Ha a cikk olvasója úgy véli, őt nem fenyegeti semmilyen veszély, hiszen ő „csak" egy hétköznapi kisember, akkor máris sorolhatjuk az ellenérveket. Jogosítványa, helyrajzi számmal rendelkező ingatlanja, bankkártyája valószínűleg, személyigazolványa és TAJ-száma pedig biztosan mindenkinek van. Ha valaki a nevében bankkártyát, kölcsönt igényelne a banktól, vagy a nevével visszaélve hamis vásárlásokat vagy kórházi számlákat produkálna, tudna néhány kellemetlen percet szerezni. Akadnak azonban olyanok is, akik személyes adatainkkal visszaélve vagy pénzszerzési céllal, vagy bosszúvágyból is nagyon megkeseríthetik az életünket. Pontos személyi adataink ismeretében (kiolvassák az iWiW-ről) például feladhatnak rólunk egy feljelentést az APEH-nak, benne pár százmillió forint be nem fizetett adóról – ez lehet egy személyes leszámolás a haragossal vagy netán a konkurenciával, de az ellopott pénzügyi adatok, például üzleti forgalom, áfa mértéke stb. bizonyos célközönségnek (például üzleti versenytársainknak) igazi pénzt érő információ. Nem is soroljuk a lehetőségeket, ezek beláthatatlanok. Rejtő Jenő – aki a sok vidám könyv mellett a komorabb Csontbrigádot is írta, melyben mintha előre megérezte volna a későbbi koncentrációs táborok hangulatát – azt írta, „az fél igazán a jövőtől, akinek van fantáziája".

Beszélő számok

Ha megvizsgáljuk a cikk írásakor rendelkezésre álló statisztikákat, a **www.phishtank.com** adatai szerint több mint 230 ezer adathalász oldal szerepel a nyilvántartásukban. Hasonlóan riasztóak a **www.antiphishing.org** számai is: a phishing esetek száma szinte minden évben megduplázódik. A célpontok döntő hányada bank vagy pénzintézet, 4-5 százaléka kiskereskedelmi egység, és körülbelül 1 százaléka internetszolgáltató (ISP) vagy egyéb vállalkozás. Földrajzilag is érdekes a kép: itt az USA, Kína és Oroszország követi egymást – ezek a billentyűleütés-naplózó (keylogger) és trójai letöltők által használt és az adott országban hosztolt webhelyekre utalnak.

A Symantec 2006 második félévéről szóló jelentésében pedig Izrael bizonyult az internetes támadások melegágyának, második Tajvan, őket követik az Egyesült Államok és Lengyelország. Ez persze nem okvetlenül az elkövetők nemzetiségét jelöli, hanem csupán a rosszindulatú kódokat futtató gépek helyszínére utal. Az újabb összefoglaló tanúsága szerint az interneten keresztül végrehajtott támadások döntően továbbra is az Egyesült Államokból indulnak, a második helyen e tekintetben Kína áll, és meglepetésre Oroszország kiszorult az első tízből, a harmadik helyen Németország váltotta fel. Papp Péter információbiztonsági szakértő novemberi sajtótájékoztatóján hangzott el az az érdekes adat, miszerint a bűnözőknek nagyon is kifizetődő az elektronikus csalásokkal foglalkozni, hiszen 2005-ben ebből már több pénzük származott, mint a drogkereskedelemből. A számítógépes csalásokkal okozott kár az USA-ban elérte a 105 milliárd dollárt.



Az adathalász akcióknak sosincs uborkaszezonja, de a piros betűs ünnepek közeledtével mindig fellendül a csalási kedv

Még a legjobb biztonsági szoftver sem segít, ha személyesen ki tudják kémlelni jelszavunkat

„Az óvatosság nem bizalmatlanság” (Virág elvtárs)

Mit tudhatok? Mit kell tennem? Mit szabad remélnem? Ezekre a kérdésekre igyekszünk most felvázolni néhány hasznos tanácsot.

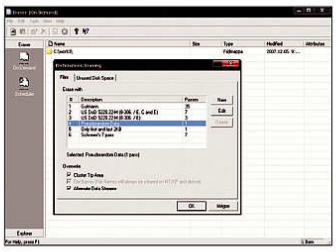
• Az internet használatakor a számítógép védelme érdekében a lehető legnagyobb gondossággal járjunk el; az esetleges vírusfertőzésekkel, betörési kísérletekkel és trójai programokkal szemben védjük rendszerünket tűzfallal, víruskeresővel és kémprogramirtóval.

• Rendszeresen töltsük le az általunk használt operációs rendszerhez, böngészőhöz, víruskeresőhöz, és egyéb szoftverekhez az elérhető frissítéseket, javítóverziókat és csomagokat.

• Mások jelenlétében, illetve nyilvános helyen (például internetkávézó, munkahelyen sokak által közösen használt gép stb.) ne vegyünk igénybe banki internetes szolgáltatást.

• Használjunk kellően erős (nem saját vagy családtagjaink nevét, hanem kis- és nagybetűket, valamint egyéb karaktereket is tartalmazó, továbbá tíz karakter hosszúság feletti) jelszavakat, és ezeket rendszeres időközönként, például negyedévente cseréljük.

• Gyanú esetén tekintsük úgy, mintha jelszavaink máris illetéktelen kezekbe kerültek volna, és haladéktalanul változtassuk meg őket – biztos, ami biztos alapon.



Az ingyenes Erase segédprogram hatásosan segít eltüntetni a nemkívánatos adatokat eladásra váró használt gépünkről

• Ne legyünk lusták, és minden helyszínen más, egyedi jelszót válasszunk. Kevés szánalmasabb és elkeserítőbb dolog van, mint ha valakinek mindenhol ugyanaz a jelszava, és amikor azt ellopják, rövid úton a banki, levelezési, web-, FTP-, üzenő- és iWiW-kapcsolatait is szétdúlják – rosszabb esetben illetéktelenül felhasználják a nevükben.

• Fontos vagy bizalmas adatokat tartalmazó nyomtatott vagy kézzel írt papírjainkat ne dobjuk egy darabban a szemetesbe, hanem lehetőség szerint saját kezűleg semmisítsük meg őket valamilyen módon (iratdaráló, égetés, apró darabokra tépkedés stb.).

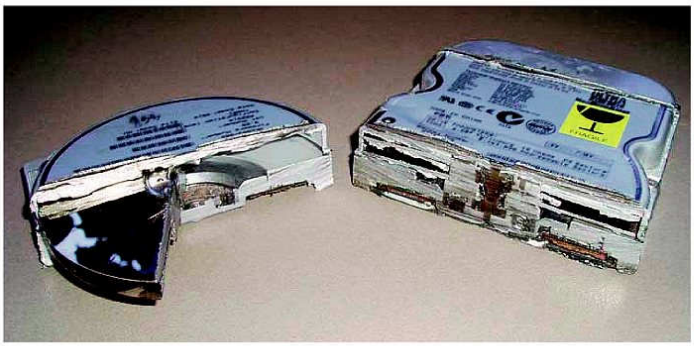
• Fontos vagy bizalmas adatokat tartalmazó adathordozóinkat (hajlékonylemez, CD, DVD) ne dobjuk ki egyszerűen a szemetesbe, hanem célszerű saját kezűleg megsemmisíteni őket (például késsel vagy csavarhúzóval karcoljuk össze a felületét, törjük szét).

• Ha eladjuk korábban használt adathordozóinkat (merevlemez, USB-háttértár, memóriakártya, belső memóriával ellátott digitális fényképezőgép, iPod), ne csak egyszerűen töröljük annak tartalmát, mert az adatok különféle adat-helyreállító célprogramokkal egyszerűen visszaállíthatók. Lehetőség szerint saját kezűleg írjuk felül semmitmondó adatokkal, vagy használjunk többszörös alapos törlést végző segédprogramot (például Eraser, DBAN, Secure Erase), és csak ezt követően adjuk tovább őket. A működésképtelen merevlemezt akár saját kezűleg is megsemmisíthetjük, ehhez dobjuk tűzbe, fűrészeljük ketté, vagy fúrjuk át fúrógéppel.

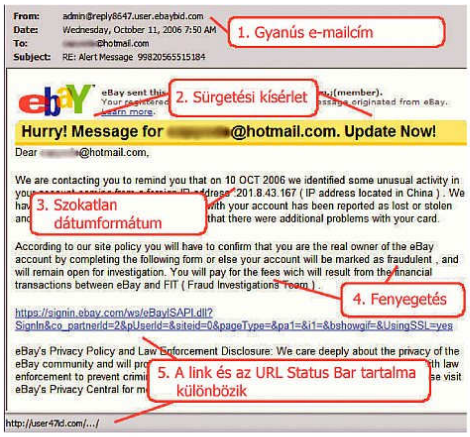
• Lejárt bankkártyánkat vagy más, műanyag alapú azonossági igazolványunkat kidobás előtt alaposan semmisítsük meg: égessük el, vagy vágjuk szét egészen kis darabokra.

• Ha az utcán vagy bárhol adathordozót (CD/DVD, USB-kulcs stb.), vagy iPodot találunk, legyünk gyanakvóak! Hátha pont nekünk készítették oda, akár egy újfajta billentyűzetleütés-naplózó (keylogger) vagy más kémprogram is lapulhat rajta. Ez a módszer nagyon népszerű vezető beosztású emberek elleni célzott kémkedésre.

A védelem alapja a jó minőségű vírus- és kémirtó, egy jó tűzfallal megtámogatva, az okos heurisztika pedig segít távol tartani az újabb trójai és egyéb kártékony programokat



„Mire vágsz fel, öreg? Darabokra!” – mégpedig szó szerint. Nem árt tudni, hogy a szervizekben a cseregaranciára leadott hibás merevlemez bárhová kerülhet: javítják, újra eladják, esetleg szakszerűtlenül egyszerűen kidobják a szemétbe



A hivatalos helyről érkező levelekben sosincs ilyesmi

akad. Használjunk neves, a teszteken jól teljesítő, ismert, illetve megbízható és elérhető hivatalos gyártótól származó víruskeresőt, amelyhez magas színvonalú terméktámogatás is jár.

Persze a szűkebb szakma is ötleteket merít a fórumok hasábjain, íme az ezekből kimazsolázott két legérdekesebb hozzászólás:

• Ha frissen felfedezett, még nem letiltott adathalász oldalra tévedünk, érdemes ott gyorsan feltölteni a rubrikákat szemét adatokkal, hogy az adathalászoknak a felgyülemlett adatbázisból nehezebb legyen kinyerni a valódi áldozatok adatait. Mivel ezeket úgyis eladják (mármint a begyűjtött adatokat), hátha megér előbb-utóbb pár törött lábat a sok hibás adat.

• Bankkártyánkra érdemes tollal rárírni egy teljesen rossz PIN-kódot, hogy az esetleges tolvaj esélye erősen limitálódjon (időben és a kísérletek számában).

Ahogy Obi-Wan Kenobi fogalmazott: „Harcolni sokféleképp lehet”. Ha ellenünk is ezt teszik, nem csukhatjuk be a szemünket, nekünk is változnunk, tanulnunk, figyelnünk kell, és meg kell ismerni az ellenséget.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK, KIADVÁNYOK

Secunia Software Inspector:
secunia.com/software_inspector/
David Manning filmje a spamről:
www.imdb.com/title/tt0936499/
www.rootkit.com
www.phishtank.com/stats.php
www.virushirado.hu
www.biztonsagportal.hu
wigwam.info
virusirto.lap.hu
www.antiphishing.org/
www.shadowserver.org
www.heidi.ie/eraser/
Kevin Mitnick:
A megtévesztés művészete
Kevin Mitnick:
A behatolás művészete
Dr. Kürti Sándor:
Az Infostrázsa
Nemere István:
Csalók könyve